Tecnologie Satellitari e Sicurezza: lo Spazio come nuova frontiera cyber

Spazio e Cybersecurity: verso una strategia Italiana?

Alberto Tuozzi:

Agenzia Spaziale Italiana - Responsabile Rapporti con l'Unione Europea

Fondazione E.Amaldi - Presidente

L’arma cyber nello spazio

Il più grande attacco informatico dall'inizio della guerra in Ucraina

Viasat KA-SAT Satellite In Europe Still Under Attack In 2023

May 16, 2023

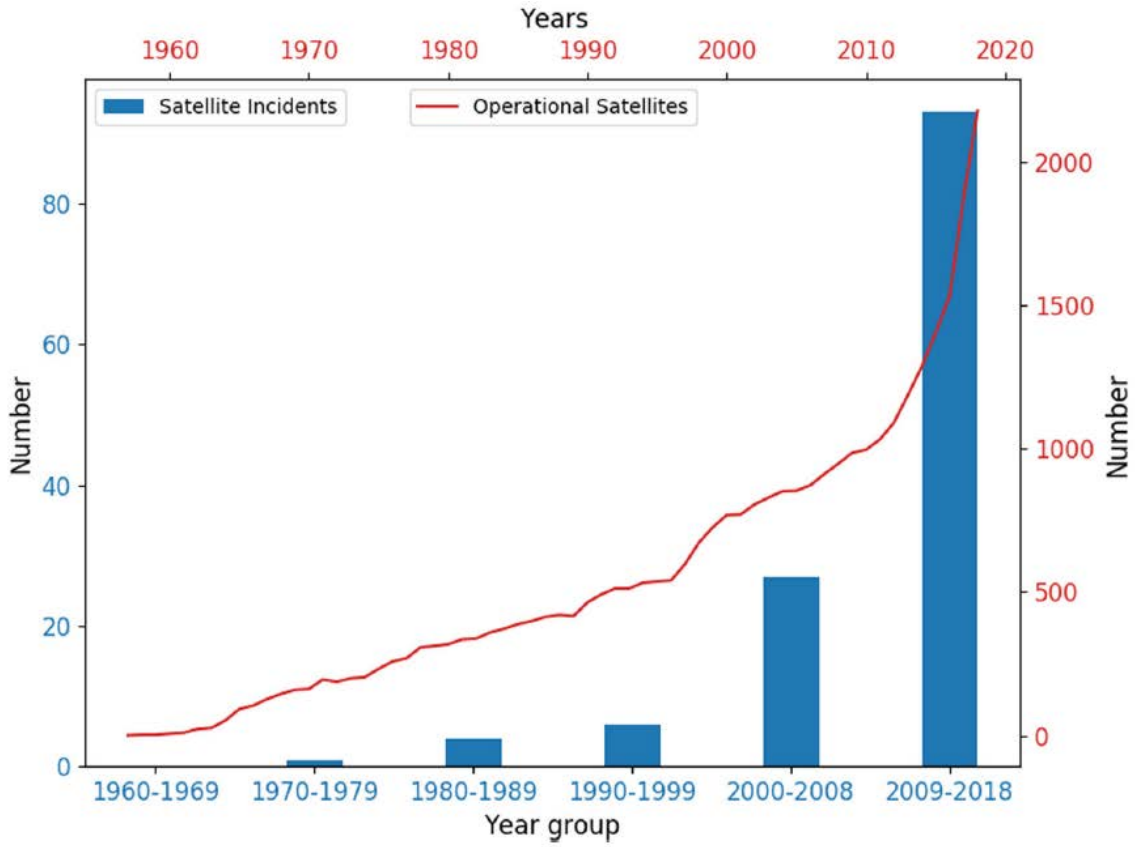
Russia Targets Elon Musk's Starlink Satellites Over Ukraine Help; SpaceX Counters Attack Faster Than US Military: Pentagon

CISA researchers: Russia’s Fancy Bear infiltrated US satellite network

We breached Russian satellite network, say pro-Ukraine partisans

Ukraine, Team OneFist brings cyber warfare against Russia into Space

Dati statistici di attacchi resi noti (1977-2019)



Source: Presentazione ESA Space Meeting Veneto 2023

Cyber & Spazio

- Le infrastrutture spaziali sono complesse, interconnesse e strategiche
- Supportano (e sono!) delle infrastrutture critiche e strategiche
- Supportano (e forniscono!) servizi critici e strategici

Le minacce

- Command Injection
- Payload Control
- Denial of Service
- Advanced/Custom Malware

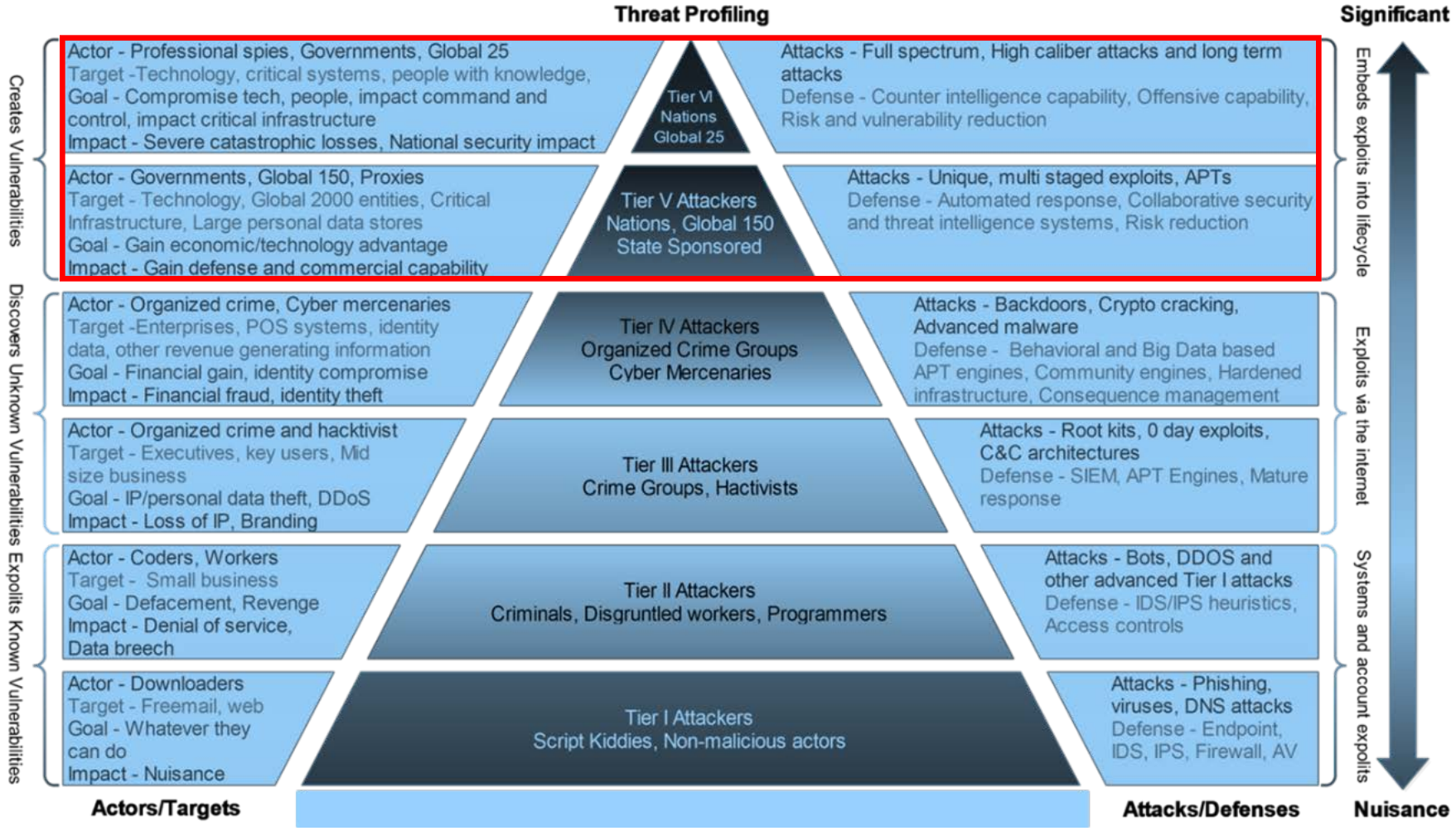
- Command Injection
- Spoofing
- Replay attack
- Denial of Service

- Spoofing
- Denial of Service
- Misconfiguration
- Malware
- Common IT Threats

- Infrastructure Hacking
- Hijacking
- Malware
- Denial of Service
- Common IT Threats

Non va sottovalutato il fattore dell'obsolescenza!

Gli attori


Threat Profiling
Significant
Actor - Professional spies, Governments, Global 25
Target -Technology, critical systems, people with knowledge,
Goal - Compromise tech, people, impact command and control, impact critical infrastructure
Impact - Severe catastrophic losses, National security impact
Tier VI Nations Global 25
Attacks - Full spectrum, High caliber attacks and long term attacks
Defense - Counter intelligence capability, Offensive capability, Risk and vulnerability reduction
Actor - Governments, Global 150, Proxies
Target - Technology, Global 2000 entities, Critical Infrastructure, Large personal data stores
Goal - Gain economic/technology advantage
Impact - Gain defense and commercial capability
Tier V Attackers Nations, Global 150 State Sponsored
Attacks - Unique, multi staged exploits, APTs
Defense - Automated response, Collaborative security and threat intelligence systems, Risk reduction
Actor - Organized crime, Cyber mercenaries
Target -Enterprises, POS systems, identity data, other revenue generating information
Goal - Financial gain, identity compromise
Impact - Financial fraud, identity theft
Tier IV Attackers Organized Crime Groups Cyber Mercenaries
Attacks - Backdoors, Crypto cracking, Advanced malware
Defense - Behavioral and Big Data based APT engines, Community engines, Hardened infrastructure, Consequence management
Actor - Organized crime and hacktivist
Target - Executives, key users, Mid size business
Goal - IP/personal data theft, DDoS
Impact - Loss of IP, Branding
Tier III Attackers Crime Groups, Hactivists
Attacks - Root kits, 0 day exploits, C&C architectures
Defense - SIEM, APT Engines, Mature response
Actor - Coders, Workers
Target - Small business
Goal - Defacement, Revenge
Impact - Denial of service, Data breech
Tier II Attackers Criminals, Disgruntled workers, Programmers
Attacks - Bots, DDOS and other advanced Tier I attacks
Defense - IDS/IPS heuristics, Access controls
Actor - Downloaders
Target - Freemail, web
Goal - Whatever they can do
Impact - Nuisance
Tier I Attackers Script Kiddies, Non-malicious actors
Attacks - Phishing, viruses, DNS attacks
Defense - Endpoint, IDS, IPS, Firewall, AV
Creates Vulnerabilities
Discovers Unknown Vulnerabilities
Exploits Known Vulnerabilities
Embeds exploits into lifecycle
Exploits via the internet
Systems and account exploits
Actors/Targets
Attacks/Defenses
Nuisance

Le minacce emergenti nel mondo spaziale

- Denial of service Attacks performed at RF level in the downlink, uplink or ground infrastructures
- Attacks to the crypto system via Quantum computers
- Side channel and tempest attacks to the receiver
- Viruses or trojans in the receivers
- Network cyberattacks to the ground networks
- Laser weapons and Electro magnetic pulse (EMP) weapons in space
- Tempest attacks satellite to satellite
- Rogue ground transmitter

Tecniche emergenti di mitigazione dei rischi

- Signal intelligence detection on board satellites and on ground
- Definition and integration of post quantum algorithms
- Integration of Quantum communications and Quantum Key Distribution (QKD) mechanism
- Tempest and anti tamper protection for receivers
- Intelligent anti virus and threat detection based on Artificial Intelligence
- RF shielding from tempest attacks and EMP weapon
- Two-way authentication of ground and satellite transmitters.

Cosa è necessario fare?

Formazione & Awareness

Limitare gli incidenti di sicurezza dovuti alla mancanza di conoscenza e sensibilità nei confronti della cybersecurity.

Direttive & Standard

Sviluppare normative che prevedano il supporto allo sviluppo e l'implementazione di iniziative e standard che tengano conto delle specificità del settore.

Supply Chain

Includere processi e controlli che tengano conto delle minacce cyber in tutta la catena di sviluppo degli assetti e dei programmi spaziali.

Operazioni

L'aggiornamento, l'assessment ed il monitoraggio continuo dei sistemi consentono di mantenere alta la sicurezza verso l'evolversi delle minacce.

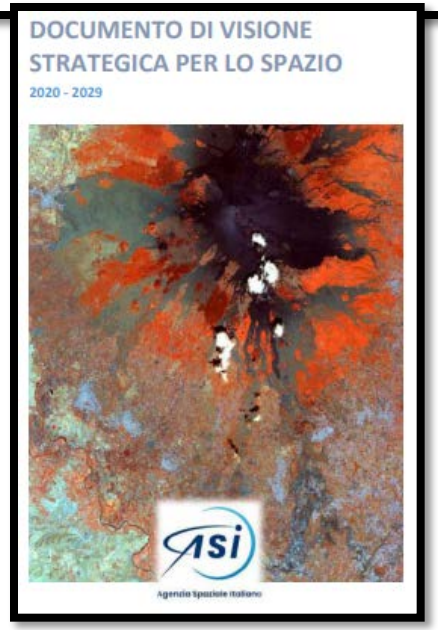
Aspetti chiave per una Strategia a livello Europeo

- Aumentare la sicurezza del segmento spazio
  - Prevenire, monitorare e rispondere alle minacce
- Uso dello spazio per aumentare la sicurezza e la difesa della terra
- Sicurezza dei sistemi spaziali lungo tutta la catena di produzione e le fasi di sviluppo
- Investimenti in ricerca e sviluppo
- Aumento della sovranità tecnologica
  - Ridurre dipendenze (anche da alleati)
  - Sicurezza nella catena di fornitura dei prodotti
  - Sinergie con altri programmi Europei e nazionali

Dove siamo?

Presidenza del Consiglio dei Ministri

Strategia nazionale di sicurezza per lo spazio



NIS 2 additional sectors

- FOOD
- MANUFACTURING
- POSTAL & COURIER
- PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR SERVICES
- ICT SERVICE MANAGEMENT
- WASTE WATER
- WASTE MANAGEMENT
- PUBLIC ADMINISTRATION
- SPACE
- RESEARCH
- CHEMICALS

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 30 luglio 2020, n. 131

Art. 3.

Settori di attività

1. Ai fini dell'inclusione nel perimetro, sono oggetto di individuazione, in applicazione del criterio di gradualità di cui all'articolo 1, comma 2, del decreto-legge, in via prioritaria, fatta salva l'estensione ad altri settori in sede di aggiornamento, i soggetti operanti nel settore governativo, concernente, nell'ambito delle attività dell'amministrazione dello Stato, le attività delle amministrazioni CISR, nonché gli ulteriori soggetti, pubblici o privati, operanti nei seguenti settori di attività, ove non ricompresi in quello governativo:

a) interno;
b) difesa;
c) spazio e aerospazio;
d) energia;
e) telecomunicazioni;
f) economia e finanza;
g) trasporti;
h) servizi digitali;
i) tecnologie critiche, di cui all'articolo 4, paragrafo 1, lettera *b)*, del Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio del 19 marzo 2019, con esclusione di quelle riferite ad altri settori di cui al presente articolo;
l) enti previdenziali/lavoro.

Conclusioni

- Qualsiasi assetto spaziale è critico per la sicurezza
  - Anche un cubesat compromesso rappresenta una grave minaccia
- Lo spazio diventa sempre più «accessibile»
  - Si moltiplicano gli attori commerciali
  - Ma anche le minacce

- Una strategia nazionale per la cybersicurezza dello spazio
  - Che sviluppi elementi di strategia per la cybersicurezza dello spazio
  - Che consideri le peculiarità della filiera spaziale nazionale
  - Che sia in linea con la strategia per la sicurezza e la difesa dello spazio

Grazie!